NOTICE OF ALLOWANCE

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on January 29, 2007 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner. The examiner notes that the submission of the Swedish Patent document 517116 does not include a translation, the submission has not been considered by the examiner.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with James LaBarre on June 18, 2010.

The application has been amended as follows:

On page 1 of the specification, after line 2, insert the section header "Field of the Invention";

On page 1 of the specification, after line 7, insert the section header “Background of the Invention”;

On page 4 of the specification, after line 11, insert the section header “Summary of the Invention";

On page 5 of the specification, after line 10, insert the section header “Brief Description of the Drawings”;

On page 6 of the specification, on line 1, insert the section header “Detailed Description of the Invention";

On page 6 of the specification, lines 16-22 have been amended as follows:

XJVML describes a simplistic architecture based on the virtual processor JVML0 defined in the document by R. Stata and M. Abadi entitled "A Type System for Java Bytecode Subroutines" published in the reference document SRC Research Report 158 on Jun. 11, 1998. ~~and available at the following electronic address:~~

~~http://www.research.digital.com/SRC/~~

25. (Currently Amended) ~~An~~ A portable electronic object, ~~wherein it implements claim 1~~ that executes a program P supplied by a non-secure other electronic object in the form of a succession of F instructions, where F denotes the number of instructions of the program P, said portable electronic object being configured to perform the following stages of operatons:

a) an initialization stage during which the portable electronic object generates an ephemeral key K, then receives from the other electronic object the program P, the number of instructions F and a program identifier ID corresponding to a hashing of P, computes the hash h of the program P with a $HASH_1$ function, by using a compression function H_1 and a constant IV_1, and generates signatures σ_i, by means of a symmetrical cryptographic MAC function and the key K, which signatures σ_i the portable electronic object transmits to the other electronic object;

b) an execution stage during which the portable electronic object checks that h and ID are equal, and verifies that ID is stored in its non-volatile memory, and then requests, one after the other, the instructions of P so as to execute them, and, for at least some of them, performs a verification sub-stage that includes requesting a signature σ constructed on the basis of the signatures σ_i generated during the initialization stage and, by means of a $HASH_2$ function defined by a compression function H_2 and a constant IV_2, verifies said signature σ; and

c) a reaction stage that takes place whenever a signature σ is not valid.

Allowable Subject Matter

4. Claims 1-26 are allowed.

5. The following is an examiner's statement of reasons for allowance:

It was not found to be taught in the prior art of a secret-key protocol co-operating with an ephemeral secret key K; a symmetrical cryptographic MAC function .mu..sub.K co-operating with a hash function HASH.sub.1 defined by a compression function H.sub.1 and a constant IV.sub.1, and with a hash function HASH.sub.2 defined by a compression function H.sub.2 and a constant IV.sub.2; anda program identifier ID stored in the electronic object X.mu.P and corresponding to hashing of P; wherein said public-key protocol comprises the following stages: a) an initialization stage during which the X.mu.P generates an ephemeral key K, then receives from the XT the set of programs P, the number of instructions F and its identifier ID, computes the hash h of said program P with the HASH.sub.1 function, by using the compression function H.sub.1 and the constant IV.sub.1, and finally generates signatures .sigma..sub.i, by means of the .mu..sub.K function and of the key K, which signatures .sigma..sub.i it transmits to the XT; b) an execution phase during which the X.mu.P checks that h and ID are equal, also verifies that ID is stored in its non-volatile memory, and then requests, one after the other, the instructions of P so as to execute them, and, for some of them, performs a sub-stage of verification that consists in requesting a signature .sigma., constructed on the basis of the signatures .sigma..sub.i generated during the initialization stage and by means of the HASH.sub.2 function, and in verifying said signature .sigma.; c) a reaction stage that takes place whenever a signature .sigma. is not valid.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Thursday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 517-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2431